CLAIMS

What is claimed is:

1   1.   A method of establishing a secured communication session across a remote network

2   connection, comprising:

3   (a)   receiving a first certificate that includes a first digital signature;

4   (b)   obtaining a first public key;

5   (c)   using the first public key to verify the first digital signature;

6   (d)   if the first digital signature in (c) is successfully verified, receiving a second

7   certificate that includes a second digital signature;

8   (e)   obtaining a second public key; and

9   (f)   using the second public key to verify the second digital signature.

1   2.   The method of claim 1 wherein said first and second digital signatures are signed with

2   different private keys.

1   3.   The method of claim 1 wherein said second certificate includes at least a portion of said

2   first certificate.

1   4.   The method of claim 1 wherein (c) includes decrypting a portion of said first certificate to

2   recover a first hash value.

1   5.   The method of claim 4 wherein (c) also includes computing a hash of at least a portion of

2   said first certificate to produce a first computed hash value.

1   6.   The method of claim 5 wherein said first hash value is compared to said first computed

2   hash value.

1   7.   The method of claim 6 wherein (c) further includes determining said first digital signature

2   is successfully verified if said first hash value matches said first computed hash value.

1   8.   The method of claim 1 wherein (f) includes decrypting a portion of said second certificate

2   to recover a second hash value.

1   9.   The method of claim 8 wherein (f) also includes computing a hash of at least a portion of

2   said second certificate to produce a second computed hash value.

1   10.   The method of claim 9 wherein said second hash value is compared to said second

2   computed hash value.

1   11.   The method of claim 10 further including successfully verifying said second digital

2   signature if said second hash value matches said second computed hash value.

1   12.   A method of establishing a secured communication session across a remote network

2   connection, comprising:

3   (a)   receiving first and second certificates that include first and second digital

4   signatures, respectively;

5   (b)   obtaining first and second public keys;

6   (c)   using the first public key to verify the first digital signature;

7   (d)   if the first digital signature in (c) is successfully verified, verifying the second

8   digital signature; and

9   (e)   permitting the communication session to occur if both said first and said second

10   digital signatures are successfully verified.

1   13.   The method of claim 12 wherein said first and second digital signatures are signed with

2   different private keys.

1   14.   The method of claim 12 wherein said second certificate includes at least a portion of said

2   first certificate.

1   15.   The method of claim 12 wherein (c) includes using said first public key to decrypt a portion

2   of said first certificate to recover a first hash value.

1   16.   The method of claim 15 wherein (c) also includes computing a hash of at least a portion of

2   said first certificate to produce a first computed hash value.

1   17.   The method of claim 16 wherein (c) includes comparing said first hash value to said first

2   computed hash value.

1   18.   The method of claim 17 wherein (c) further includes determining that said first digital

2   signature is successfully verified if said first hash value matches said first computed hash value.

1   19.   The method of claim 12 wherein (c) includes decrypting a portion of said second certificate

2   to recover a second hash value.

1   20.   The method of claim 19 wherein (c) also includes computing a hash of at least a portion of

2   said second certificate to produce a second computed hash value.

1   21.   The method of claim 20 wherein (c) includes comparing said second hash value to said

2   second computed hash value.

1   22.   The method of claim 21 further including successfully verifying said second digital

2   signature if said second hash value matches said second computed hash value.

1   23.   A method of creating a remotely verifiable certificate, comprising:

2   (a)   retrieving a first signed certificate;

3   (b)   combining together said first signed certificate with other values;

4   (c)   computing a hash of the combination from (b); and

5   (d)   signing said hash from (c) with a private key.

1   24.   The method of claim 23 wherein said other values in (b) includes an IP address.

1   25.   The method of claim 23 wherein said other values in (b) includes a domain name.

1   26.   A computer, comprising:

2   a processor; and

3   a memory coupled to said processor;

4   wherein said memory includes storage for a first certificate and a second certificate, said

5   second certificate derived from said first certificate.

1   27.   The computer system of claim 26 wherein said processor combines at least a portion of said

2   first certificate with additional values, computes a hash of said combination, and encrypts said hash

3   with a private key.

1   28.   The computer system of claim 27 wherein said additional values include an IP address.

1   29.   The computer system of claim 27 wherein said additional values include a domain name.

1   30.   The computer system of claim 26 wherein said first certificate includes a serial number.

1   31.   The computer system of claim 26 wherein said first certificate is not created by the server.

1   32.   A client system, comprising:

2   a processor; and

3   a memory coupled to said processor; and

4   a connection to a communication link to a server;

5   wherein said processor requests a first certificate from the server, verifies a first digital

6   signature associated with said first certificate, and if said first digital signature is

7   successfully verified, requests a second certificate from said server and verifies a

8   second digital signature associated with said second certificate.

1   33.   The client system of claim 32 wherein the client uses two different public keys to verify the

2   first and second digital signatures.

1   34.   A client system, comprising:

2   a processor;

3   a memory coupled to said processor; and

4   a connection to a communication link to a server;

5   wherein said processor requests a first certificate and a second certificate from the server,

6   verifies a first digital signature associated with said first certificate, and if said first

7   digital signature is successfully verified, verifies a second digital signature

8   associated with said second certificate.

1   35.   The client system of claim 34 wherein the client uses two different public keys to verify the

2   first and second digital signatures.